

STATE OF FLORIDA)
) ss.
COUNTY OF PALM BEACH)

AFFIDAVIT

I, William S. Wiltse, being first duly sworn on oath, hereby depose
and say:

1. I am a former police detective for the City of Salem, Oregon. I worked as a police officer in the State of Oregon for 18 years, during which time I conducted criminal investigations into the sexual abuse and exploitation of children. I am currently sworn as a reserve deputy sheriff with the Palm Beach County Sheriff's Office in Palm Beach County, Florida.
2. I am the developer of the law enforcement computer application known as "Peer Spectre". This application was created in conjunction with Flint Waters of the Wyoming Division of Criminal Investigations as part of an investigative effort formerly known as Peer Precision. This effort, now known as the Child Protection System (CPS), focuses on the development of software tools to identify computers trading files depicting the sexual abuse of children and training law enforcement officers in their use. The Child Protection System was developed by TLO, LLC, a private company located in Boca Raton, Florida. I am currently employed as the Director of Law Enforcement Programming at TLO and oversee all development activities related to the aforementioned Child Protection System. I am also



certified as an instructor for the Child Protection System and regularly provide instruction to law enforcement officers prior to providing them access to the system.

3. The Child Protection System and related applications are only made available to specifically trained and licensed law enforcement officers and their use is restricted to only those law enforcement officers in the performance of law enforcement activity.
4. As part of a basic CPS "peer to peer" course, law enforcement investigators are taught the process of downloading freely available file-sharing software from the Internet and using that software to locate files depicting child sexual abuse on the Gnutella file-sharing network. This process begins by typing in descriptive text as key words and allowing the software to conduct a search of the network for files containing those key words. Officers are taught to use search terms, which are known by experienced investigators to return a greater than average number of files depicting the sexual abuse of children. Once offending files have been identified, the Internet Protocol, or IP addresses of the computers sharing those files are submitted to law enforcement servers located within the office of TLO in Boca Raton, Florida.
5. The software created for the Child Protection System was designed to replicate the process taught to investigators in their basic peer-to-peer training. Using a list of known key words, CPS software submits those as search terms on file sharing networks in the same fashion as freely

available software tools. The computers present on the these file sharing networks respond to these CPS requests in the same way they respond to any other program capable of operating on those networks. Included in those responses, participating computers provide their IP addresses, which are subsequently logged into the law enforcement database.

6. All components of the Child Protection System, to include the Peer Spectre application, function within established protocols of the file sharing networks on which they operate. All content received from participating computers is the result of requests sent to these computers using aforementioned protocols. None of the CPS software tools receive data beyond that which individual users make publicly available on these networks.
7. All computers actively connected to the Gnutella network communicate in a request / response manner. Every Gnutella message must adhere to a pre-defined structure, which is freely and publicly documented in the Gnutella network protocol. Any request that does not conform to this standard will be ignored by every other computer operating on the Gnutella network. For this reason, there is no way for an application such as Peer Spectre to "search" the entirety of a Gnutella-connected computer's contents or perform any other intrusive operation. The application simply sends a Gnutella "query" message to the receiving computer, consisting only of the keyword requested. It is the Gnutella software installed and running on the receiving

computer that performs a search within shared folders for that keyword and provides a pre-defined response.

8. Child Protection System software tools are copyrighted computer applications for which the source code has never been distributed. The source code is not distributed with the CPS software that is provided to trained law enforcement officers. Without the source code, it is not possible to authenticate the function of the application or validate its "calibration". Investigators do not receive the source code for CPS tools as part of their training, but only the applications themselves. Officers are taught how to validate the findings of the CPS system by conducting similar searches on the Gnutella network using freely available software applications.
9. The source code used by the Child Protection System is not accessible by the use of any of its related applications.
10. The source code used by the Child Protection System and related applications has not been, and will not be, distributed to any law enforcement officer or agency, to include Special Agent Melissa De La Rosa or Special Agent Nicolas Marquez of the Department of Homeland Security, Immigration and Customs Enforcement.
11. When Child Protection System applications are run, they submit lead information automatically into a law enforcement server located at TLO. There are no configuration options in any of the programs to prevent this from occurring. Only trained and licensed law enforcement investigators

receive the Child Protection System applications and they understand that the leads generated are from other licensed investigators running the application. To distribute this application to untrained and unlicensed persons would be a violation of the terms of use and compromise the training points already delivered to hundreds of investigators across the country.

12. Child Protection System applications submit all criminal lead information via the Internet to a single server by referencing a specific web address or Uniform Resource Locator (URL). This web location is not disclosed during training, but is programmed directly into the source code of the application. Users of Child Protection System applications cannot modify this address directly, but could easily expose it by using freely available network interrogation software. To distribute the application to untrained and unlicensed, non-law enforcement users could expose this web address, thereby making the law enforcement server located at TLO susceptible to digital interrogation or attack.
13. In addition to exposing the web address, distributing Child Protection System related applications could expose the format in which they communicate with the law enforcement server located at TLO. This knowledge could be used for nefarious purposes, allowing untrained and unlicensed non-law enforcement persons to submit false information into the law enforcement server. This act would not only create false leads for

investigators, but could also implicate an innocent person's IP address as participating in the collection, manufacture or distribution of child exploitation files.

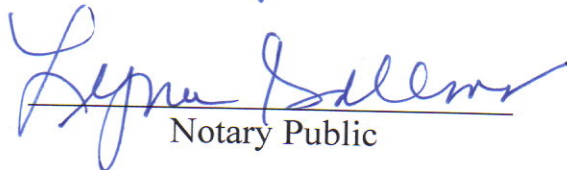
14. The Child Protection System applications have been deployed since 2009 and are currently being used by investigators throughout the United States and around the world. Based on leads these applications generate, hundreds of search warrants have been written resulting in the rescue of many children. Since the release of the Child Protection System and related applications, I am not aware of any problems affecting the reliability of the data they collect.



William S. Wiltse

I, Lynn Dallmer, a Notary Public of the County and State aforesaid, hereby certify that William Wiltse personally known to me to be the affiant in the foregoing affidavit, personally appeared before me this day and having been by me duly sworn deposes and says that the facts set forth in the above affidavit are true and correct.

Witness my hand and official seal this the 11th day of Apr., 2013.


Notary Public

My Commission expires:

